

DIRMM**U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF THE SECRETARY****DOT H 1350.2****May 1998****Chapter 14-3****SUBJ: ELECTRONIC MAIL POLICY**

1. **PURPOSE.** This chapter establishes policy and responsibilities on the use of electronic mail (e-mail) systems within the Department of Transportation (DOT).
2. **SCOPE.** This chapter covers DOT electronic mail systems used by its employees and contractor support personnel.
3. **REFERENCES.**
 - a. Computer Fraud and Abuse Act of 1986 (18 USC 1001 note, 1030).
 - b. Computer Security Act of 1987 (15 USC 271 note, 272, 278g-3, 278g-4, 278h; 40 USC 759, 759 note).
 - c. Electronic Communications Privacy Act of 1986 (18 USC 1367, 2232, 2510, 2510 notes, 2511 to 2521, 2701, 2701 note, 2702 to 2711, 3117, 3121, 3121 note, 3122 to 3127).
 - d. Freedom of Information Act (5 USC 552 et seq.).
 - e. Federal Records Act of 1950 (44 USC 2101 et seq., 2501 et seq., 2701 et seq., 2901 et seq., 3101 et seq.).
 - f. Federal Records Disposal Act (44 USC 3301 et seq.).
 - g. Paperwork Reduction Act of 1995 (5 USC Chapter 35).
 - h. Privacy Act of 1974 (5 USC 552a, 552a note).
 - i. 18 USC 2071 "Concealment, Removal, or Mutilation Generally."
 - j. Executive Orders 12674 and 12731 "Principles of Ethical Conduct of Government Officers and Employees," 5 CFR Part 2635 "Standards of Ethical Conduct for Employees of the Executive Branch," 5 CFR Chapter L and 49 CFR Part 99 "Supplemental Standards of Ethical Conduct for Employees of the Department of Transportation."
 - k. 36 CFR Chapter XII, Subchapter B-Records Management.
 - l. DOT H 1350.2 Information Systems Security Policy, DOT H 1350.250 "DOT Information Systems Security (ISS) Guide," DOT H 1350.251 "DOT Network Security Guide."

4. DEFINITIONS.

- a. **DOT users.** DOT users are individuals authorized to use e-mail as part of their assigned official duties. This includes DOT employees and support contractor personnel using DOT supplied resources.
- b. **Electronic mail.** Information created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, that may be transmitted with the message.
- c. **Electronic mail system.** A computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or data bases on computers, and word processing documents not transmitted on an e-mail system.
- d. **Record.** A record includes all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. (Federal Records Act, 44 USC 3101 et seq.).
- e. **Recordkeeping system.** A system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.
- f. **System of records.** A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to the individual.

5. GOALS.

- a. E-mail communications will be conducted in a seamless, efficient and cost-effective manner to:
 - 1) Increase productivity and information sharing;
 - 2) Improve timeliness of service to DOT users and customers;
 - 3) Facilitate and strengthen mission and program performance;
 - 4) Provide for the dissemination of public information on a timely basis, on equitable terms; and

- 5) Enhance the utility of the information to the public and other government entities.
- b. DOT e-mail systems will be developed in a manner that:
 - 1) Enables e-mail communications governmentwide and with the public;
 - 2) Uses standard protocols;
 - 3) Provides appropriate security;
 - 4) Enables a user-friendly interface;
 - 5) Builds upon existing systems; and
 - 6) Ensures system reliability and integrity.

6. POLICY.

a. General.

- 1) DOT e-mail systems are the property of the federal government. DOT owns the data stored on these e-mail systems, including all e-mail messages, even those deemed personal by their authors.
- 2) Proper uses of DOT e-mail systems include exchange of information that supports the DOT mission, goals, and objectives, job-related professional development for DOT management and staff, and communications and exchange of information intended to maintain job currency or gain additional knowledge that is directly or indirectly related to job functions.
- 3) Improper uses of DOT e-mail systems include:
 - a) Use for any purpose that violates any laws.
 - b) Concealment or misrepresentation of names or affiliations in e-mail messages.
 - c) Unauthorized access, alteration of source or destination addresses of e-mail, or misrepresentation of DOT e-mail systems and the messages contained therein.
 - d) Initiating actions which interfere with the supervisory or accounting functions of the system, including attempts to obtain "system" privileges.
 - e) Causing congestion of DOT e-mail systems by such things as the propagation of chain letters, broadcasting inappropriate messages (e.g., unsolicited personal views on social, political, religious, or other non-business matters) to lists or individuals, etc.
 - f) Use for any commercial purposes, for financial gain, or in support of "for profit" activities.

- g) Engaging in any activity that would discredit DOT, including seeking, transmitting, collecting, or storing defamatory, discriminatory, obscene, harassing, or intimidating messages or material.
 - h) Use for posting to external newsgroups, bulletin boards, or other public forums, unless it is a business-related requirement and appropriate office approvals have been obtained.
- 4) E-mail is provided to DOT users for business use. DOT e-mail systems may be used for incidental personal purposes provided that such use does not:
 - a) Directly or indirectly interfere with DOT e-mail services;
 - b) Burden DOT with noticeable incremental cost; or
 - c) Interfere with DOT user's employment or other obligations to the Government.
- 5) Standards of ethical conduct and appropriate use apply to the use of DOT e-mail systems.
- 6) The fact that information is produced or preserved electronically does not confer on it any status that is different from the same information in hard copy.
- 7) Proper business etiquette should be maintained when communicating via e-mail. When writing e-mail, DOT users should be as clear and concise as possible and avoid remarks, expressions, or attempts at humor which could be misconstrued or misinterpreted. E-mail communications should resemble typical professional/respectful business communications.
- b. **Records Management.** E-mail messages determined to be records shall be managed in accordance with federal regulations pertaining to adequacy of documentation, recordkeeping requirements, records management responsibilities, and records disposition.
- c. **Access.**
 - 1) Freedom of Information. E-mail messages are subject to public disclosure in accordance with the Freedom of Information Act (FOIA).
 - 2) Privacy.
 - a) DOT e-mail systems shall not be used to send or receive records subject to the Privacy Act of 1974 without ensuring appropriate security and privacy protection policies and safeguards are in place.
 - b) Unauthorized establishment of e-mail systems of records is prohibited.
 - c) Privacy Act system(s) of records notice(s) shall be published in the Federal Register for any new system that results from or is related to the use of e-mail.

- d) E-mail, including all messages sent or received on DOT e-mail systems, is subject to monitoring (i.e., communications in process of transmission, records in storage pending receipt, and records in archival storage by or on behalf of the user), by appropriate personnel for business purposes to:
 - i. Maintain security of the system;
 - ii. Carry out records management responsibilities;
 - iii. Conduct authorized law enforcement surveillance or investigations, including tracking unauthorized access to a DOT e-mail system;
 - iv. Conduct business during a crisis if an employee is absent when information is required;
 - v. Conduct business during a prolonged absence of an employee, when information in the employee's e-mail is required;
 - vi. Maintain national security; or
 - vii. Ensure compliance with policy set forth in paragraph 6.a.

d. **Security.**

- 1) DOT e-mail systems shall provide for security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information contained in the e-mail system.
- 2) DOT e-mail systems that meet the definition of general support system or major application (see Appendix III to OMB Circular A-130-Security of Federal Automated Information Resources) shall have a corresponding system security plan.
- 3) Security controls shall be reviewed when modifications are made to DOT e-mail systems.
- 4) New or significant changes to DOT e-mail systems that meet the definition of general support system or major application shall not be instituted without the cognizant IT security official ensuring agreement with the applicable security plan.

e. **Legal Rights.** DOT e-mail systems shall not be used in a manner which infringes upon the intellectual property of others.

f. **Litigation.** DOT e-mail communications are subject to discovery in judicial or administrative proceedings.

7. **RESPONSIBILITIES.**

a. **DOT Users are responsible for:**

- 1) Adhering to prescribed DOT e-mail policies and procedures;

- 2) Informing current and potential customers of the existence of e-mail and of other ways of communicating with DOT;
- 3) Contacting the appropriate Records Management Officer (RMO) to ensure all records retention requirements are being met; and
- 4) Consulting with appropriate personnel (e.g., records managers, FOIA officials, Privacy Act officers, security managers, legal staffs, etc.) on e-mail issues.

b. Records Management Officers (RMOs) are responsible for:

- 1) Conducting periodic reviews of electronic mail systems. The purpose of the review is to identify electronic records in each system and ensure the records are scheduled.
- 2) Establishing a training program for users of electronic mail systems that provides for the management of electronic messages as records.

c. E-Mail Administrators are responsible for:

- 1) Ensuring interconnectivity and interoperability with DOT, government, and public e-mail systems;
- 2) Assigning e-mail addresses that conform with DOT's directory infrastructure;
- 3) Distributing approved DOT e-mail policies to DOT users;
- 4) Broadcasting departmentwide e-mail messages;
- 5) Providing awareness training for DOT users on:
 - a) Proper use of electronic mail systems; and
 - b) Appropriate security measures;
- 6) Working with the cognizant RMO to develop records retention and disposition requirements for e-mail messages;
- 7) Developing and implementing audit trails to detect both authorized and unauthorized access and user compliance with DOT e-mail policies and procedures;
- 8) Implementing and maintaining appropriate security features and controls;
- 9) Conducting routine tests of e-mail system performance;
- 10) Testing and documenting the reliability of e-mail systems;
- 11) Creating and maintaining comprehensive system documentation on all aspects of system design, implementation, maintenance, and oversight; and
- 12) Ensuring timely termination of e-mail accounts and access privileges of departing DOT users.

d. **Departmental Officers and Heads of Operating Administrations are responsible for:**

- 1) Defining proper uses of e-mail beyond those contained in this policy as appropriate.
- 2) Promoting the use of e-mail in ways that achieve DOT organization strategic/outcome goals and improve service to the public.
- 3) Sharing with employees new ways to improve performance through the use of e-mail.
- 4) Enabling e-mail initiatives to be integrated with DOT efforts to reengineer business processes.
- 5) Identifying opportunities for improving interactions with other government organizations, industry, academia, and the general public through the use of e-mail.

e. **The DOT Chief Information Officer (CIO) is responsible for:**

- 1) Issuing policy on the use of e-mail within the U.S. Department of Transportation.
- 2) Defining standards (e.g., IMAP, MIME, POP, SMTP, TCP/IP, X.400, X.500, etc.) for DOT e-mail systems to ensure interoperability and interconnectivity.

8. REQUESTS FOR INFORMATION. Information concerning e-mail policy may be addressed to the Office of the Chief Information Officer (S-80).

9. DISTRIBUTION. This chapter is electronically distributed to Departmental Offices and Operating Administrations via e-mail and is available on the DOT CIO Homepage (<http://cio.ost.dot.gov>).